

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/25464 A1

(51) International Patent Classification⁷: **G06F 15/16**

(21) International Application Number: PCT/US01/29571

(22) International Filing Date:
20 September 2001 (20.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/668,035 21 September 2000 (21.09.2000) US

(71) Applicant: **OMEGA WEB INC.** [US/US]; 1126 Broadway, Burlingame, CA 94010 (US).

(72) Inventor: **WANG, Alvin**; 920 Oakes Street, E. Palo Alto, ca 94303 (US).

(74) Agents: **GLENN, Michael** et al.; Glenn Patent Group, 3475 Edison Way, Ste. L., Menlo Park, CA 94025 (US).

(81) Designated States (*national*): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

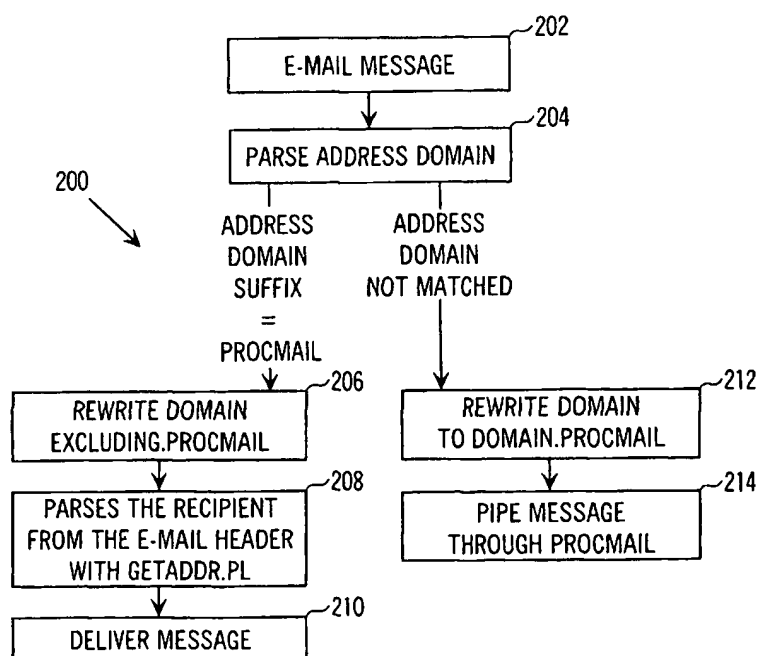
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

- with international search report
- with amended claims

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: E-MAIL SPAM ELIMINATION METHOD AND SYSTEM



(57) Abstract: An e-mail system includes an address book (108) that registers all e-mail correspondents wishing to send messages (202) to a particular user recipient. All e-mail directed to the user from outside is blocked unless the sender is registered in the address book and has a valid token (200). A limited number of such tokens are issued to each correspondent, and only after the sender has satisfactorily disclosed their identity. Such tokens limit the amount of access to a recipient. If the recipient later decides that any such sender is, in fact, a spammer, then any further e-mail from that sender can be blocked.

WO 02/25464 A1

E-MAIL SPAM ELIMINATION METHOD AND SYSTEM

5

Background Of The Invention

Technical Field

10 The present invention relates to electronic mail (e-mail), and more specifically to methods and systems for controlling the delivery of unwanted e-mail messages (spam).

Description Of The Prior Art

15 Unwanted e-mail, or spam, is becoming a great nuisance. Spammers are becoming more adept at being annoying and getting around ordinary filters. One way they do this is to hide their real e-mail sending address and plug in some phony one. They then use a new return e-mail address for every new piece of spam. Although every spammer is ultimately trying to sell something, they all seem to prevent a simple e-mail reply.

20 Instead, you must go to a website or call a phone number where you must listen to a long recorded message and leave a voice-mail message.

More advanced e-mail filters are able to recognize keywords and phrases in the subject and message body, and then use the occurrence of these in a new message to block

25 out the whole message. For example, "get rich quick" or "buy now" appearing in the subject line could signal an unwanted message. Eudora is an example of an e-mail application that includes a highly developed user-programmable filter.

But such filters can also block messages from desirable correspondents, so great care

30 must be used in the selection of the keywords and phrases. A monitor also needs to be setup so the blocked messages can be reviewed to make sure acceptable

messages are not being filtered out. Systems like that described by Lucent Technologies (Murray Hill, NJ) in European Patent Application EP-0-899-918-A2, "System and method for providing anonymous remailing and filtering of electronic mail", published 03.03.1999, strip away the real source's address in e-mails and render the
5 messages sent anonymous. Prior art filters can do little to stop such trickery.

The general problem with conventional spam eliminators is they must know something about the spammer and their messages in order to block them. Spammers use this weakness to their advantage by constantly finding subjects, messages, and return e-
10 mail addresses that seem inoffensive.

European Patent Application EP-0-813-162-A2, published 17.12.1997, titled "Method and apparatus for identifying and discarding junk electronic mail", depends on a group of trusted users to collectively determine what is junk e-mail. Once a piece is labeled as
15 junk e-mail, unviewed copies in the e-mail systems of the other trusted users are immediately disposed of. Single users thus get far less junk e-mail, especially in large organizations. However, someone must get stung first before the e-mail is blocked entirely by the system. A very similar approach is repeated in United States Patent 6,052,709, titled "Apparatus and method for controlling delivery of unsolicited electronic
20 mail", which was issued April 18, 2000, to Sunil Paul.

Two filters are used in the method and system described by William B. McCormick, et al., in United States Patent 6,023,723, issued Feb. 8, 2000. A first filter is supplied with e-mail sender addresses the user does not want to receive messages from. A second
25 filter is loaded with those e-mail sender addresses that the user does want to receive. Messages caught by the first filter are simply dumped. Messages recognized by the second filter are passed through for delivery. Messages from addresses not brought to the attention of either filter are forwarded to a "waiting room" for the user to look at later. Any messages in this waiting room that are later rejected by a user's review are gleaned

for information that is forwarded to a central system. A master-list update is then compiled for the first filters of all users/subscribers.

5

Summary Of The Invention

10

An e-mail system includes an address book that registers all e-mail correspondents wishing to send messages to a particular user recipient. All e-mail directed to the user from outside is blocked unless the sender is registered in the address book and has a valid token. A limited number of such tokens are issued to each correspondent, and only after the sender has satisfactorily disclosed their identity. Such tokens limit the amount of access to a recipient. If the recipient later decides that any such sender is, in fact, a spammer, then any further e-mail from that sender can be blocked.

15

Brief Description Of The Drawings

20

Fig. 1 is a top-level flowchart of an e-mail server embodiment of the present invention;
Fig. 2 is a flowchart of the Sendmail subroutine of Fig. 1;
Fig. 3 is a flowchart of the Procmail subroutine of Fig. 1;
Fig. 4 is a flowchart of the PERL script "asptest.pl" subroutine of Fig. 1;
Fig. 5 is a flowchart of the PERL script "dumpit.pl" subroutine of Fig. 1;
Fig. 6 is a flowchart of the PERL script "getaddr.pl" subroutine of Fig. 1; and
Fig. 7 is a flowchart for creating user accounts in an embodiment of the present invention.

25

Detailed Description Of The Invention

Fig. 1 represents an e-mail server embodiment of the present invention, and is referred to herein by the general reference numeral 100. A new e-mail message 102 enters a

sendmail subroutine 104 which inspects the "from" address header included in the e-mail. The whole e-mail is either then forwarded to a deliver-message subroutine 106 or a procmail subroutine 108, depending on whether the sender is an acceptable and known correspondent who has been preregistered in the system. Procmail 108 calls on
5 an asptest.pl subroutine 110, a dumpit.pl subroutine 112, and a getaddr.pl subroutine 114, to process the incoming e-mails for acceptability to the user. PERL-script implementations are preferred, as indicated by the ".pl" extensions mentioned herein for the subroutine files. Some of the processed e-mails can be returned by procmail 108 to sendmail 104 for ultimate delivery to the user.

10

Fig. 2 details a sendmail subroutine 200 which is similar to the sendmail subroutine 104 (Fig. 1). A new e-mail message 202 is passed on to an address domain parser 204. The "from" address header in the message received is checked to see if the domain matches a preregistered domain, e.g., one that is known to the user or the e-mail
15 system. If the domain does match a preregistered domain, and has a suffix of ".procmail", a step 206 strips the address of the ".procmail" suffix. A step 208 parses the e-mail recipient header e.g., with getaddr.pl subroutine 114, and delivers the e-mail in a step 210. If the message is from an unknown source, e.g., the domain does not match any preregistered domain, the "from" address header is rewritten in a step 212 as
20 "domain.procmail" and the whole message is piped through procmail by a step 214.

Fig. 3 details a procmail subroutine 300 which is similar to the procmail subroutine 108 (Fig. 1). A new e-mail message 302 is passed on to a step 304 which generates a proper "from" address header. A step 306 checks for an "x-loop:" header entry. If one
25 is not found, a step 308 makes a copy of the message and sends it to the asptest.pl subroutine 110. If the test in the asptest.pl subroutine returned a "no", then the message is dumped in a step 310 that trashes it with dumpit.pl subroutine 112. But if the test in the asptest.pl subroutine returned a "yes", then the message is forwarded to a step 312. Such parses the recipient field from the e-mail header by calling the

getaddr.pl subroutine 114. A step 314 then bounces the message on to the recipient/user.

Fig. 4 details an asptest.pl subroutine 400 which is similar to the asptest.pl subroutine 110 (Fig. 1). A new e-mail message 402 is passed on to a step 404 which parses the sender and recipient info from the e-mail message header. Such parsed-out address information is then used by a step 406 to generate a hypertext transfer protocol (HTTP) message. This is then sent to an active server pages (ASP) application running on a webserver, e.g., WINDOWS-NT with IIS. Such http-message can be communicated over any network, especially over the Internet via TCP/IP. A centralized system would then be possible that could be used to share preregistration information and any information generated about spammers.

The webserver's ASP typically responds with one of four commands amounting to, (a) "deliver the e-mail", (b) "deliver the e-mail with form attached", (c) "reply and attach error", or (d) "delete the e-mail". If the answer is anything but "deliver e-mail", an error message to the user is generated. A step 408 parses the ASP response. A step 410 generates an exitcode from the ASP response, and a step 412 returns the error message to procmail subroutine 108 and exits. Procmail uses the exitcode and error message to decide whether to "deliver the e-mail" or to trash it by sending it to the dumpit.pl subroutine 112. The "deliver the e-mail" choice uses the getaddr.pl subroutine 114 to parse out the recipient. The e-mail is then bounced to the recipient in step 314.

Fig. 5 details a dumpit.pl subroutine 500 which is similar to the dumpit.pl subroutine 112 (Fig. 1). A new e-mail message 502 and an error message 504 are passed on to a step 506 which is to dump the message, reply to it, or to attach a form. If the decision is to "delete the e-mail", a null step 508 simply exits without doing anything. If the decision is to "reply and attach error", a reply header is generated in a step 510. A step 512 appends the error message to the e-mail, and a step 514 sends the new e-mail. But if

the decision in step 506 is to "deliver the e-mail with form attached", a step 516 uses the getaddr.pl subroutine to parse the recipient from the e-mail header. A step 518 appends a hypertext markup language (HTML) form, and sends the e-mail to the recipient in a step 520.

5

Fig. 6 details a getaddr.pl subroutine 600 which is similar to the getaddr.pl subroutine 112 (Fig. 1). A new e-mail message 602 has its header parsed in a step 604 for its recipient information. A step 606 returns to the calling program with the recipient address.

10

Fig. 7 represents a method for creating new user accounts with the systems described in Figs. 1-6, and is referred to herein by the general reference numeral 700. The method 700 is preferably included in a business model embodiment of the present invention. A profitable business can be constructed with an implementation from Figs. 1-7 that operates over the Internet and uses HTTP, HTML, and simple mail transfer protocol (SMTP) documents with both webpage servers and mail servers. The users are required, at least initially to enroll and load preferences, to have an Internet client and browser. Such Internet client is used in step 406 to ask the ASP what to do with particular messages received. The SMTP mail server delivers the basic e-mail messages, and the webserver use the Internet to communicate filter information between users and a centralized database. Such database and webserver is operated at a profit by charging users a subscription fee or per-use fee.

20

The new user account creation method 700 begins with a fill-in form 702 that can be implemented with JavaScript and HTML-code generated by the ASP in the webserver. An information 704 includes user data that is needed to enroll a user in a system like that described in Figs. 1-6. A step 706 validates the information submitted, e.g., by rule-based checking. It confirms receipt by the provider to the newly enrolled

25

user. A step 708 downloads the verified information to the database for real-time use over the Internet.

In general, embodiments of the present invention defaults to blocking mail from all
5 unknown sources. Any e-mail from known and acceptable sources are preferably
viewable in a user directory free of unsolicited messages. Senders wishing to send
messages to recipient-users, and who are unknown, must register with a central control
system. For example, an Internet webserver is provided as a central control and
registry. Those registering must identify themselves sufficient to satisfy the system
10 operators and users. A limited number of tokens are then electronically credited to such
previously unknown senders. The limits on the number of tokens allotted prevents
mass mailings. Recipient-users who do have the sender listed as a known and
acceptable source can authorize mail delivery without requiring any tokens.

15 Messages that are sent with tokens and accepted by their intended recipients will
preferably automatically generate more tokens for use by the corresponding sender.
This is equivalent to rewards for good behavior, or the way credit is established by
establishing a record of responsible conduct. It also limits the volume of mail that can be
sent by one sender, and thus makes the sending of junk e-mail uneconomical. Any e-
20 mail received by using tokens as passports is sent to a directory in which the users know
the messages inside may be unsolicited and require validation.

A system of validation levels can be applied to authorized users. A "caller-ID" level
confirms valid "from" e-mail addresses. A second level check if the sender's physical
25 address is acceptable. A third level check if the sender's phone number is acceptable.
A fourth level check if the sender has a valid certificate. Corporate senders can also be
classified as non-profit or having paid a fee. Such fees can be collected by the system
operator, or credited to individual recipients.

Such validation levels, fee payments, non-profit senders, and the implementation of tokens can be included in the construction of the asptest.pl subroutine 110 and 400. A corresponding application program is included in the ASP program on the responsible webserver.

5

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. Accordingly, the invention should only be limited by the claims included

10 below.

Claims

1. A method for stopping unwanted messages from being accepted in an e-mail

5 delivery system, comprising:

receiving an e-mail message from a sender via an SMTP-mail server;

parsing an address header from said e-mail message with an e-mail delivery system;

10 sending an e-mail source address obtained in the step of parsing to a webserver;

checking said e-mail source address against a list of source addresses maintained in a database associated with said webserver;

instructing said e-mail delivery system from said webserver to deliver or not-deliver said e-mail message to a user;

15 displaying said e-mail message at said e-mail delivery system to said user if instructed to do so by said webserver; and

disposing of said e-mail message at said e-mail delivery system if instructed to do so by said webserver.

20 2. The method of claim 1, wherein:

the step of sending an e-mail source address depends on transmitting an HTTP-message via the Internet to an active server pages (ASP) equivalent application program operating on said webserver.

25 3. The method of claim 1, wherein:

the step of instructing said e-mail delivery system depends on transmitting an HTTP-message via the Internet from an active server pages (ASP) equivalent application program operating on said webserver.

4. The method of claim 1, further comprising the step of:

registering an e-mail source in said database such that the step of checking will approve of said e-mail message if originated by that e-mail source.

5 5. The method of claim 1, further comprising the step of:

preapproving a list of e-mail sources in said database such that the step of checking will allow delivery of said e-mail message if originated by any one of such e-mail sources.

10 6. The method of claim 1, further comprising the step of:

allowing an e-mail source to list itself in said database such that the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

7. The method of claim 1, further comprising the steps of:

15 gathering identification information from an e-mail source not registered in said database;

testing whether said identification information is acceptable according to a minimum standard; and

if acceptable, allowing said e-mail source to be listed in said database such that
20 the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

8. The method of claim 7, further comprising the steps of:

issuing a first token to an e-mail source previously not registered in said
25 database; and

requiring said first token to be expired before the step of checking will allow delivery of said e-mail message when originated by such e-mail source.

9. The method of claim 7, further comprising the steps of:

issuing a second token to said e-mail source previously not registered in said database if said user validates them after having received and read one of their e-mail messages.

- 5 10. An e-mail delivery system, comprising:
- a webserver connected to a computer data network;
- an SMTP-mail sever for providing the delivery of e-mail messages to a user;
- a spam-elimination system connected to receive said e-mail messages from the SMTP-mail server; and
- 10 a database of registered e-mail senders included in the webserver;
- wherein, the spam-elimination system transmits any e-mail source address information included in any received e-mail messages to the webserver;
- wherein; the database is consulted for a registration listing matching said e-mail source address information; and
- 15 wherein, the webserver provides for the instruction of the spam-elimination system to deliver or not deliver to a user a particular e-mail message.

11. The e-mail delivery system of claim 10, wherein the spam-elimination system further includes:

- 20 a program subroutine for receiving an e-mail message from a sender via said SMTP-mail server;
- a program subroutine for parsing an address header from said e-mail message with an e-mail delivery system;
- a program subroutine for sending an e-mail source address obtained in the step
- 25 of parsing to a webserver;
- a program subroutine for checking said e-mail source address against a list of source addresses maintained in a database associated with said webserver;
- a program subroutine for instructing said e-mail delivery system from said webserver to deliver or not-deliver said e-mail message to a user;

a program subroutine for displaying said e-mail message at said e-mail delivery system to said user if instructed to do so by said webserver; and

a program subroutine for disposing of said e-mail message at said e-mail delivery system if instructed to do so by said webserver.

5

12. The system of claim 1, wherein:

the program subroutine for sending an e-mail source address depends on transmitting an HTTP-message via the Internet to an active server pages (ASP) equivalent application program operating on said webserver.

10

13. The system of claim 11, wherein:

the program subroutine for instructing said e-mail delivery system depends on transmitting an HTTP-message via the Internet from an active server pages (ASP) equivalent application program operating on said webserver.

15

14. The system of claim 11, further comprising:

a program subroutine for registering an e-mail source in said database such that the step of checking will approve of said e-mail message if originated by that e-mail source.

20

15. The system of claim 11, further comprising:

a program subroutine for preapproving a list of e-mail sources in said database such that the step of checking will allow delivery of said e-mail message if originated by any one of such e-mail sources.

25

16. The system of claim 11, further comprising:

a program subroutine for allowing an e-mail source to list itself in said database such that the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

17. The system of claim 11, further comprising:

a program subroutine for gathering identification information from an e-mail source not registered in said database;

5 a program subroutine for testing whether said identification information is acceptable according to a minimum standard; and

a program subroutine for allowing said e-mail source, if acceptable, to be listed in said database such that the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

10

18. The system of claim 17, further comprising:

a program subroutine for issuing a first token to an e-mail source previously not registered in said database; and

15 a program subroutine for requiring said first token to be expired before the checking will allow delivery of said e-mail message when originated by such e-mail source.

19. The system of claim 17, further comprising:

20 a program subroutine for issuing a second token to said e-mail source previously not registered in said database if said user validates them after having received and read one of their e-mail messages.

¹⁴
AMENDED CLAIMS

[received by the International Bureau on 3 January 2002 (03.01.02);
original claims 1-19 replaced by new claims 1-18 (8 pages)]

REPLACEMENT CLAIMS

1. A method for stopping unwanted messages from being accepted in an e-mail delivery system, comprising:

5 receiving an e-mail message from a sender via an SMTP-mail server;
parsing an address header from said e-mail message with an e-mail delivery system;

sending an e-mail source address obtained in the step of parsing to a webserver;

10 checking said e-mail source address against a list of source addresses maintained in a database associated with said webserver;

instructing said e-mail delivery system from said webserver to deliver or not-deliver said e-mail message to a user;

displaying said e-mail message at said e-mail delivery system to said user if instructed to do so by said webserver;

15 disposing of said e-mail message at said e-mail delivery system if instructed to do so by said webserver; and

allowing an e-mail source to list itself in said database such that the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

20

2. The method of claim 1, wherein:

the step of sending an e-mail source address depends on transmitting
an HTTP-message via the Internet to an active server pages (ASP) equivalent
5 application program operating on said webserver.

3. The method of claim 1, wherein:

the step of instructing said e-mail delivery system depends on
transmitting an HTTP-message via the Internet from an active server pages
10 (ASP) equivalent application program operating on said webserver.

4. The method of claim 1, further comprising the step of:

registering an e-mail source in said database such that the step of
checking will approve of said e-mail message if originated by that e-mail
15 source.

5. The method of claim 1, further comprising the step of:

preapproving a list of e-mail sources in said database such that the
step of checking will allow delivery of said e-mail message if originated by any
20 one of such e-mail sources.

6. The method of claim 1, further comprising the steps of:

gathering identification information from an e-mail source not registered
in said database;

5 testing whether said identification information is acceptable according
to a minimum standard; and

if acceptable, allowing said e-mail source to be listed in said database
such that the step of checking will allow delivery of said e-mail message if
originated by such e-mail source.

10

7. The method of claim 6, further comprising the steps of:

issuing a first token to an e-mail source previously not registered in
said database; and

requiring said first token to be expired before the step of checking will
15 allow delivery of said e-mail message when originated by such e-mail source.

8. The method of claim 6, further comprising the steps of:

issuing a second token to said e-mail source previously not registered
in said database if said user validates them after having received and read

20 one of their e-mail messages.

9. An e-mail delivery system, comprising:

a webserver connected to a computer data network;

an SMTP-mail sever for providing the delivery of e-mail messages to a

5 user;

a spam-elimination system connected to receive said e-mail messages

from the SMTP-mail server;

a database of registered e-mail senders included in the webserver; and

means for allowing an e-mail source to list itself in said database:

10 wherein, the spam-elimination system transmits any e-mail source
address information included in any received e-mail messages to the
webserver;

wherein; the database is consulted for a registration listing matching
said e-mail source address information; and

15 wherein, the webserver provides for the instruction of the spam-
elimination system to deliver or not deliver to a user a particular e-mail
message.

10. The e-mail delivery system of claim 9, wherein the spam-elimination
20 system further includes:

a program subroutine for receiving an e-mail message from a sender via said SMTP-mail server;

a program subroutine for parsing an address header from said e-mail message with an e-mail delivery system;

5 a program subroutine for sending an e-mail source address obtained in the step of parsing to a webserver;

a program subroutine for checking said e-mail source address against a list of source addresses maintained in a database associated with said webserver;

10 a program subroutine for instructing said e-mail delivery system from said webserver to deliver or not-deliver said e-mail message to a user;

a program subroutine for displaying said e-mail message at said e-mail delivery system to said user if instructed to do so by said webserver; and

a program subroutine for disposing of said e-mail message at said e-mail delivery system if instructed to do so by said webserver.

15

11. The e-mail delivery system of claim 10, wherein:

the program subroutine for sending an e-mail source address depends on transmitting an HTTP-message via the Internet to an active server pages

20 (ASP) equivalent application program operating on said webserver.

12. The e-mail delivery system of claim 10, wherein:

the program subroutine for instructing said e-mail delivery system depends on transmitting an HTTP-message via the Internet from an active
5 server pages (ASP) equivalent application program operating on said webserver.

13. The e-mail delivery system of claim 10, further comprising:

a program subroutine for registering an e-mail source in said database
10 such that the step of checking will approve of said e-mail message if originated by that e-mail source.

14. The e-mail delivery system of claim 10, further comprising:

a program subroutine for preapproving a list of e-mail sources in said
15 database such that the step of checking will allow delivery of said e-mail message if originated by any one of such e-mail sources.

15. The e-mail delivery system of claim 10, wherein said means for allowing an e-mail source to list itself in said database comprises a program

20 subroutine for allowing an e-mail source to list itself in said database such that

the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

16. The e-mail delivery system of claim 10, further comprising:

5 a program subroutine for gathering identification information from an e-mail source not registered in said database;

a program subroutine for testing whether said identification information is acceptable according to a minimum standard; and

a program subroutine for allowing said e-mail source, if acceptable, to
10 be listed in said database such that the step of checking will allow delivery of said e-mail message if originated by such e-mail source.

17. The e-mail delivery system of claim 16, further comprising:

a program subroutine for issuing a first token to an e-mail source
15 previously not registered in said database; and

a program subroutine for requiring said first token to be expired before the checking will allow delivery of said e-mail message when originated by such e-mail source.

20 18. The e-mail delivery system of claim 16, further comprising:

a program subroutine for issuing a second token to said e-mail source previously not registered in said database if said user validates them after having received and read one of their e-mail messages.

1/4

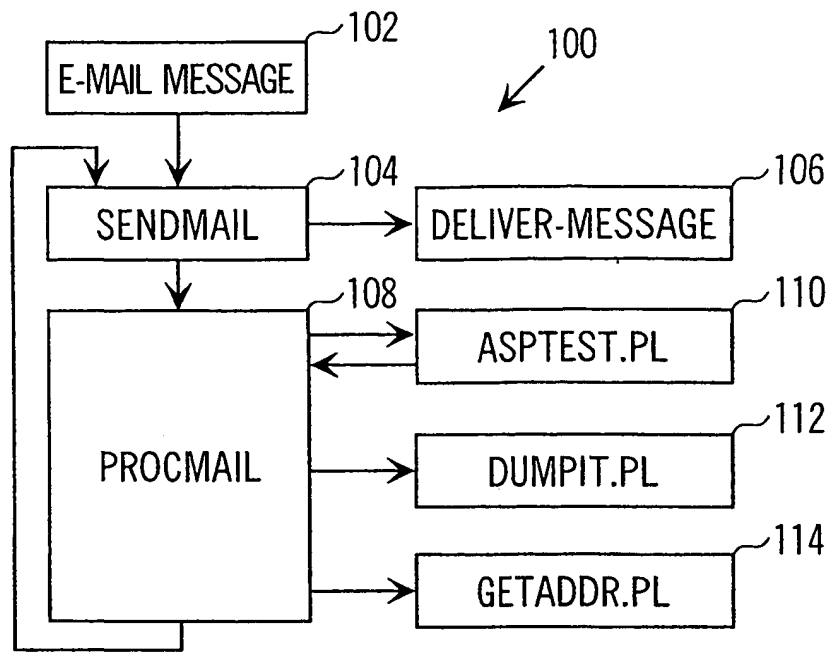


FIG. 1

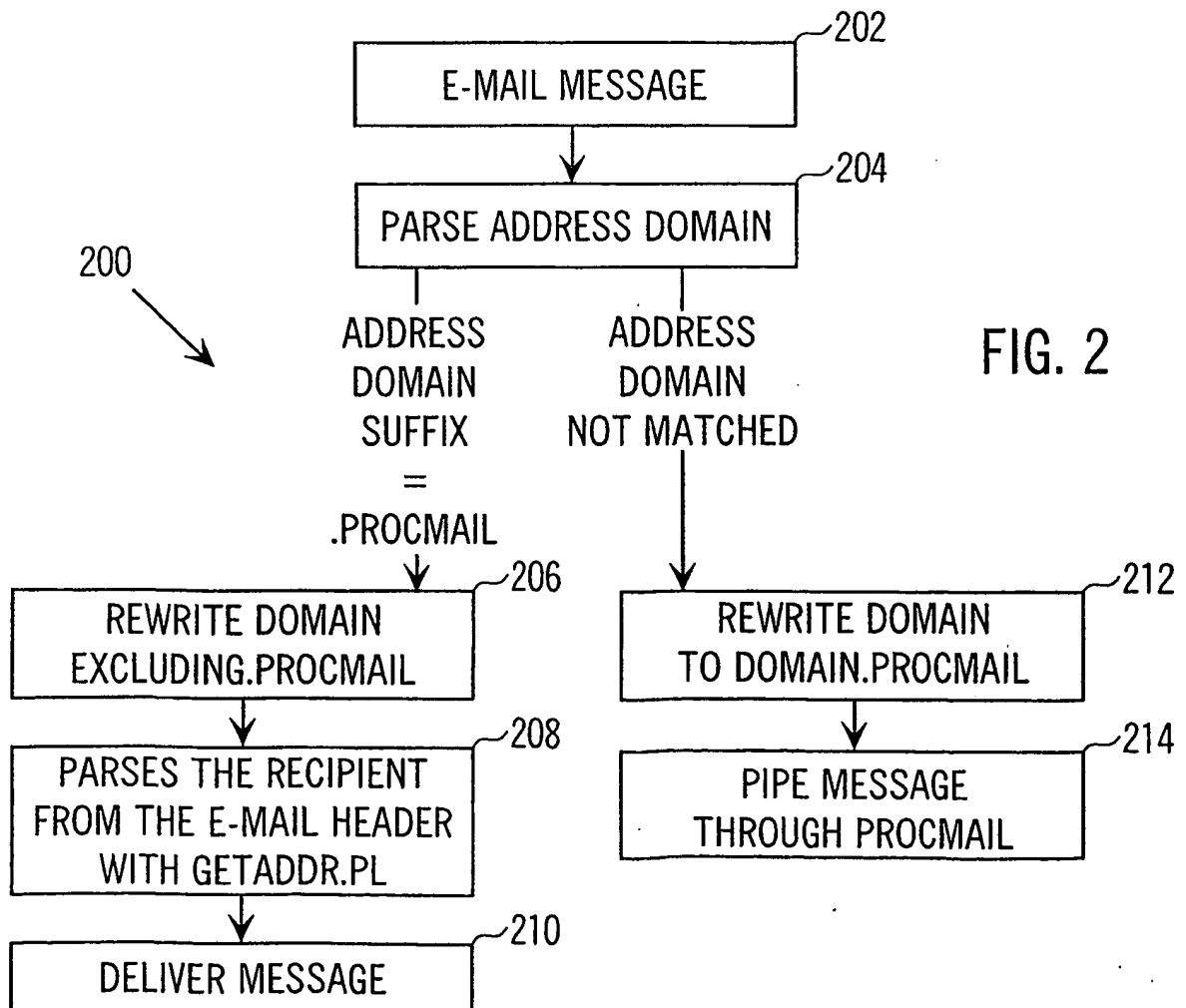


FIG. 2

2/4

FIG. 3

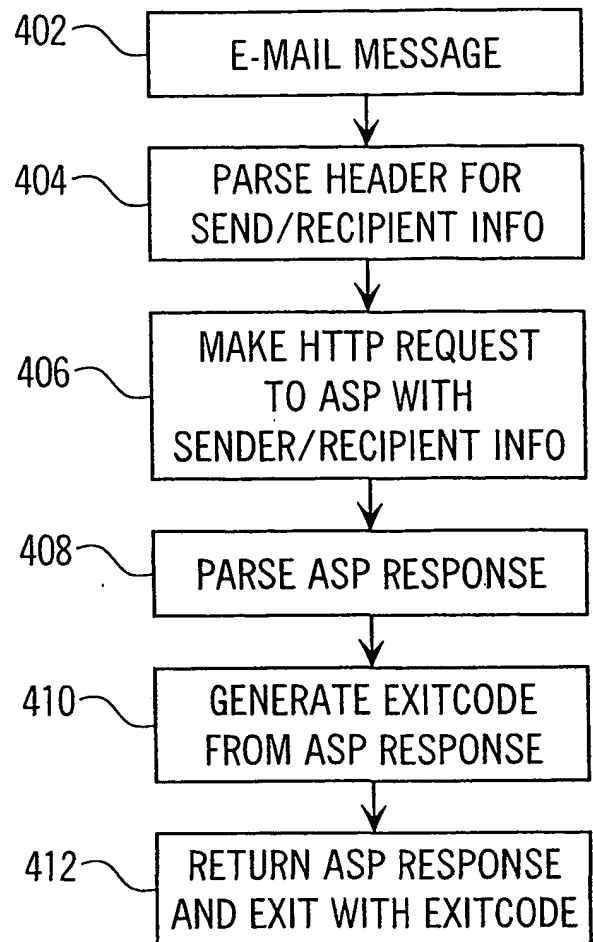
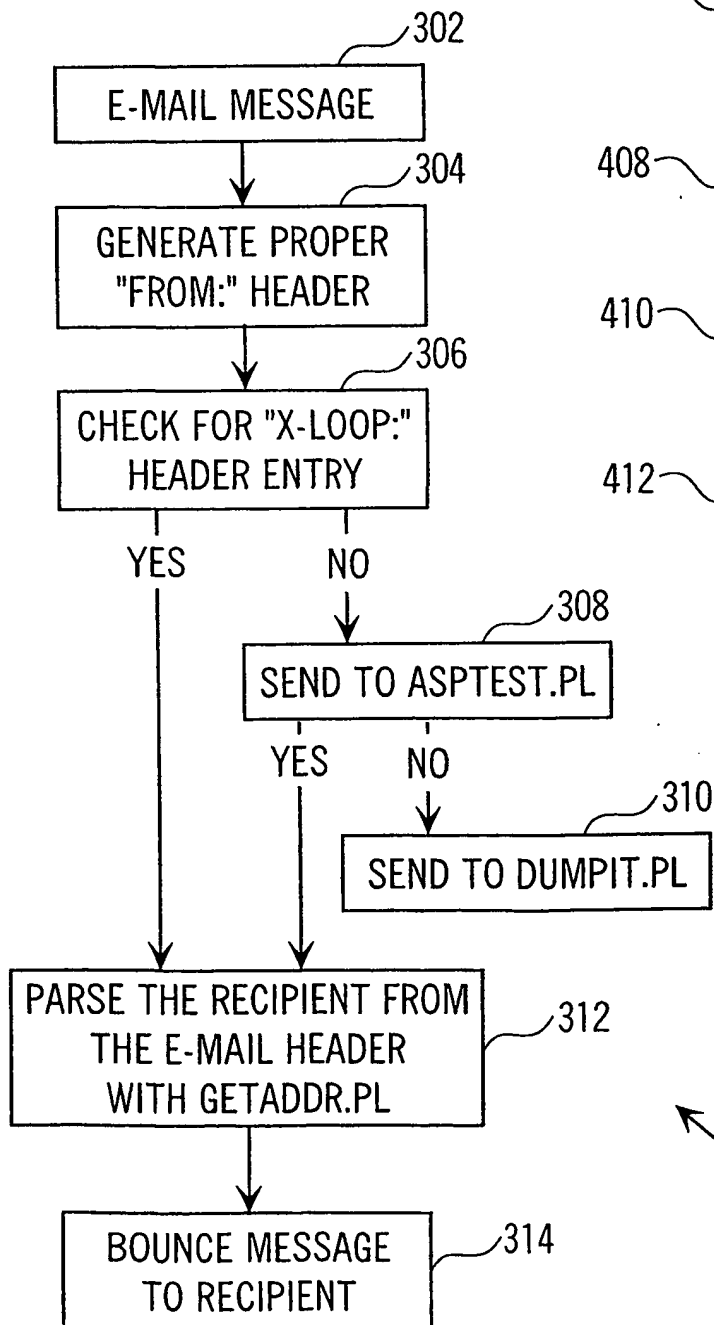


FIG. 4

3/4

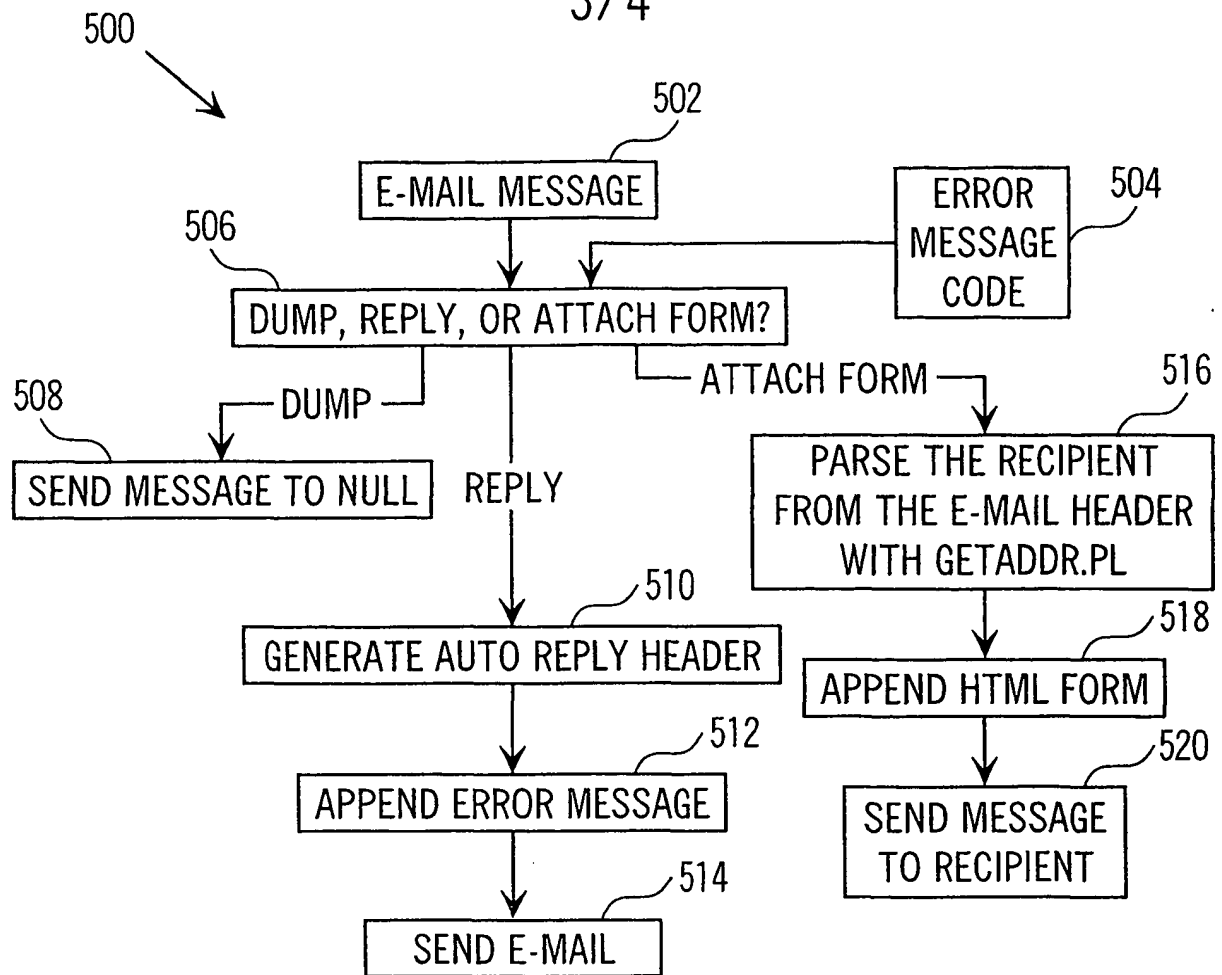


FIG. 5

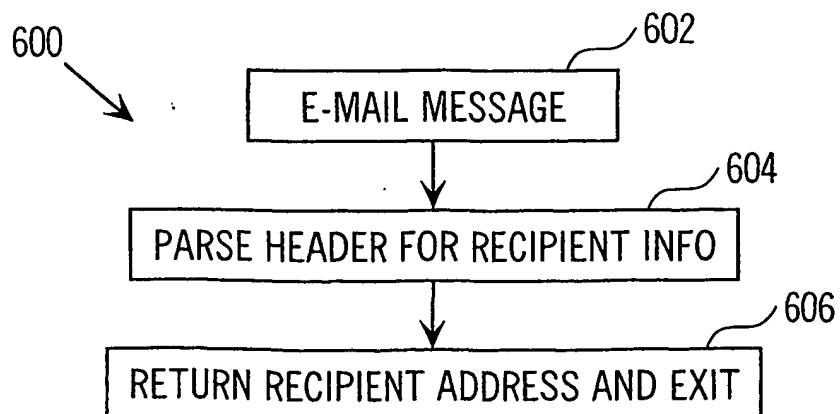


FIG. 6

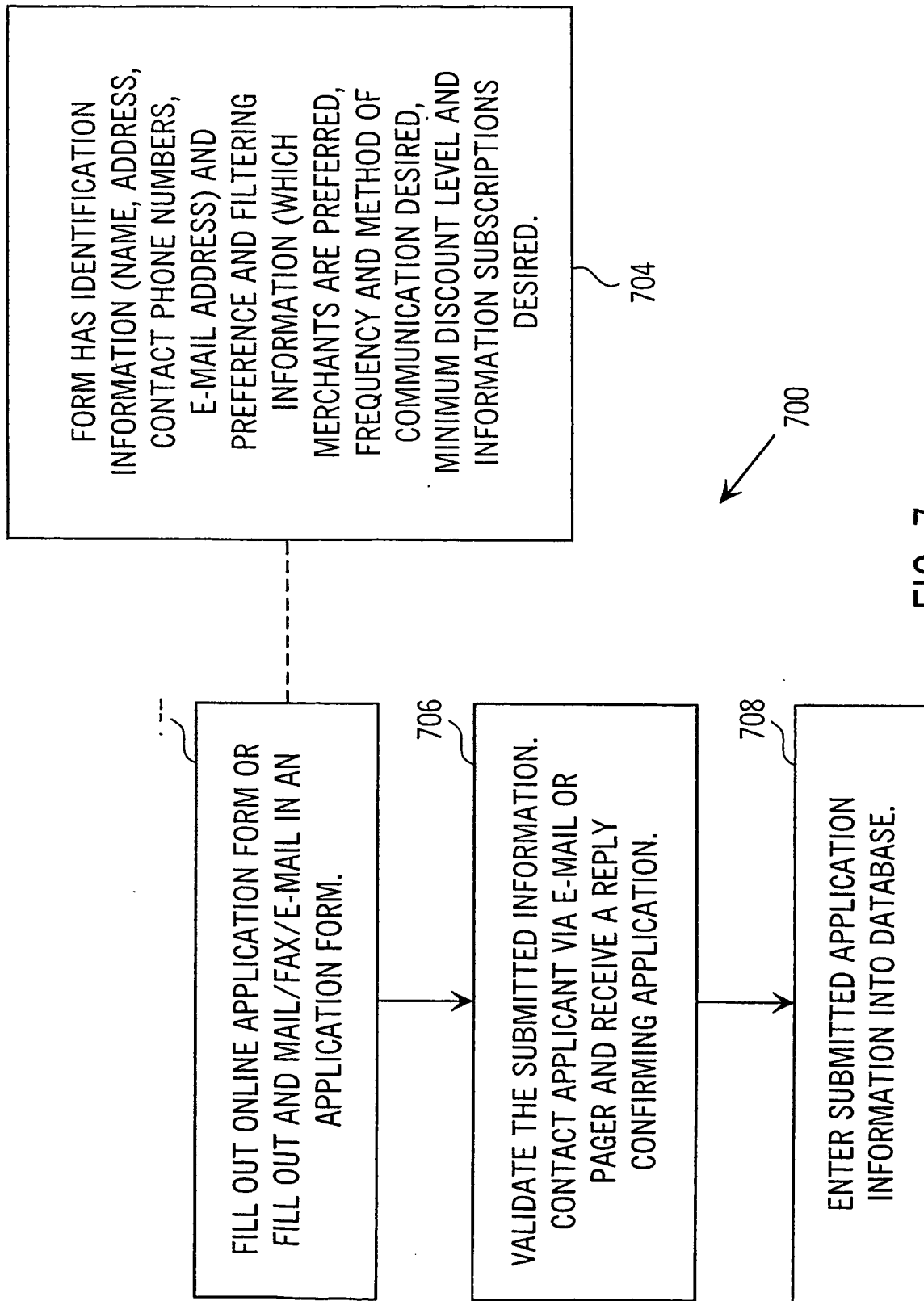


FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/29571

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/16

US CL : 709/206

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 709/206

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,023,723A (McCORMICK et al) 8 February 2000 (8.02.00), column 3, lines 20-67, column 4, lines 1-65.	1,4-7,10-11, 14-17
Y		2-3,8-9,12-13,18-19
Y	US 5,930,479A (HALL) 27 JULY 1999 (24.07.1999), column 9, lines 20-26.	2-3, 12-13
Y	US 6,266,692B1 (GREENSTEIN) 24 July 2001 (24.07.2001), column 3, lines 30-65	8-9, 18-19

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

31 October 2001 (31.10.2001)

Date of mailing of the international search report

06 NOV 2001

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703)305-3230

Authorized officer

Glen Burgess

Telephone No. 703-305-3900

Peggy Hanoel